**An Acad Bras Cienc (2020) 92(2): e20181207 DOI 10.1590/0001-3765202020181207**
Anais da Academia Brasileira de Ciências | *Annals of the Brazilian Academy of Sciences*
Printed ISSN 0001-3765 I Online ISSN 1678-2690
www.scielo.br/aabc | www.fb.com/aabcjournal

ENGINEERING SCIENCES

# Bogdanov Map-based Permuted Double Image Encryption

SUBASHINI V. JANARDHANAN & POORNACHANDRA SANJEEVA

**Abstract:** Chaos-based image encryption schemes shuffle the position of the pixels (confuse), change their values (diffuse), to camouflage the identity of the original image. In this paper, a symmetric image cryptosystem based on permutation is proposed. Permutation, used both to change the position of the pixel and modify its value, is undertaken using the Bogdanov map. First, the input image is permuted using the Bogdanov map so that the pixel positions are changed. Thereafter, the resultant scrambled image is sliced into bit-planes which are again separately subjected to the Bogdanov map. The encrypted image is constructed by encrypting the scrambled bit-planes with the key generated using dyadic transform. The experimental results exhibited random behavior in the distribution of the pixel values of the encrypted image. The cryptosystem is simple and fast, as it is permutation-based and, secure, it may be used in real-time transmission.

**Key words:** Bogdanov map, chaos, dyadic transform, image cryptosystem, permutation, symmetric.

## INTRODUCTION

The Internet has become an integral part of today's communication network. With the availability of abundant information communicated over the Internet, coupled with technological developments in the fields of visual communication and digital signal processing, there is a rapid increase in the widespread applications of digital imaging everyday. This entails security and authorized access to sensitive images such as those in the fields of medicine, defense, forensics, finance, research, etc. Consequently, with the rapid development of communication networks, there is a need to effectively protect such digital images in the open network environment. A solution to this would be to use a cryptosystem to render the information unintelligible, so an unintended recipient or intruder cannot take a chance on it. However, the traditional encryption algorithm based on the number theory may be inappropriate for digital images, given certain inherent features of these images such as large data volume, high redundancy, strong correlation among image pixels and storage characteristics. Hence, image cryptosystem has become an essential branch of cryptography. Comparatively speaking, image encryption algorithms have their own description and unique characteristics with exceptional specifications applicable to images. Chaos-based cryptosystems can provide efficient image encryption.

To resist common attacks, a cryptosystem must satisfy two basic cryptographic properties: confusion and diffusion (Alvarez & Li 2006). As stated by Shannon (Kocarev & Lian 2011),

"Diffusion means spreading out the influence of a single plaintext bit over many ciphertext bits so as to hide the statistical structure of the plaintext. Confusion refers to the use of transformations that complicate dependence of the statistics of ciphertext on the statistics of plaintext". A permutation process weakens the correlation among the pixels of the image. To secure a color watermark image from visual perception, the authors of (Agilandeeswari & Ganesan 2016), sliced the image into 24 bit-planes and permuted the pixels using the Arnold transform before embedding it into a video frame. The transform is utilized in the permutation process of the permutation-diffusion mechanism proposed by (Ye 2011). As in the case of (Ye 2011), cryptosystems proposed by (Kumar et al. 2011, Run-he et al. 2011, Zhang et al. 2012, 2014) do not require sorting to use Arnold transform-based permutation algorithms. During the process of encrypting biometric fingerprint images, (Abundiz-Pérez et al. 2014), took advantage of permutation after diffusion. An expand-and-shrink strategy to shuffle the image with reconstructed permuting plane is employed in (Zhang et al. 2013). To increase the speed of the permutation process (Guo et al. 2014) carried out a row-by-row and column-by-column permutation operation. Like the Arnold transform, the Lorenz system of equations is also noteworthy for producing chaotic solutions for certain parameter values and initial conditions and hence are used as a permutation technique (Gonzales et al. 2000, Radwan et al. 2004). Authors of (Baptista 1998, Pisarchik et al. 2006, Pisarchik & Zanin 2008, Som & Sen 2013, Sun et al. 2008) used conventional discrete chaotic maps in the permutation phase whereas (Zanin & Pisarchik 2014) used the logistic map. Instead of permuting pixels in the case of the literature above, (Al-Romema et al. 2012) permuted the bits of the pixels.

Certain authors combined chaotic and non-chaotic techniques to improve the security and robustness of their cryptosystem. For example, (Zhang & Xiao 2014) designed a cryptosystem based on a coupled logistic map, self-adaptive permutation, a substitution transform and combined global diffusion. A block cipher encryption system presented by (Abdeihaleem et al. 2014) used the Lorenz chaotic generation for the confusion process and a chess-based diffusion process. The image encryption scheme proposed by (Wu et al. 2015) used a coupled map lattice for permutation and a fractional-order Chen chaotic system for diffusion. A detailed study on symmetric encryption algorithms using chaotic and non-chaotic algorithms was done by (Radwan et al. 2016). They classified algorithms into three: substitution-only, permutation-only or both. Most of the image encryption algorithms available fall under permutation-only, the advantage of these systems being their speed of encryption. Nevertheless, the safekeeping of the information depends entirely on the confidentiality of the algorithm used. In addition, the encryption is done only by permuting the pixel positions and is prone to attacks.

To safeguard the content of transmitted images, an effectually simple chaos-based symmetric encryption algorithm that is specific for images is proposed and its performance analysed in this paper. Bogdanov map-based permutation is used to apply the idea of confusion and diffusion for images. Confusion shuffles the pixel positions within the image and results in a new organisation of pixels, while diffusion changes the values of the pixels. Experimental results show that it is simple, fast and robust.

Section, Bogdanov Map, of this paper portrays the basics of Bogdanov map. In section, The proposed cryptosystem, Bogdanov map-based permuted encryption and decryption

algorithms are discussed. Section, Results and discussion presents encryption outputs and evaluations. The section Conclusion summarizes the findings.

## MATERIALS AND METHODS

### Bogdanov map

The proposed method makes use of the Bogdanov map (Arrowsmith et al. 1993), to scramble the pixel positions in an image. The Bogdanov map is a planar quadratic map with area-preserving nature. The proposed method takes the benefit of discretization and makes use of the map's symplectic form,

$$x' = x + y' \tag{1}$$

$$y' = y + kx(x-1) \tag{2}$$

When applied to images, Eq. (1) and Eq. (2), $(x, y)$ represent the coordinate position of the pixels in the original image and $(x', y')$ is the resultant coordinates position of the pixel in the altered image and $k$ is any positive integer.

### The proposed cryptosystem

A chaos-based symmetric image cryptosystem is proposed. It is a permutation image encryption algorithm. The Bogdanov map is used to permute the image pixels. The classical confusion-diffusion architecture is adopted in the design of the proposed cryptosystem. Pixel level permutation is combined with bit level permutation and chaotic transform to attain good encryption levels.

### Image encryption

The image encryption process is shown in Figure 1. In the confusion stage of image encryption, the Bogdanov map is used to scramble (permute) the pixels of the input image, $I$. The process is repeated $m$ times to render the image unintelligible. Let the resultant image be $C_s$. As the pixel positions are exchanged, the correlation among the pixels in the input image weakens. In the diffusion stage, $C_s$ is sliced into eight bit-planes, $B_i$, $1 \le i \le 8$. These eight bit-planes are subjected to the Bogdanov map separately in such a way that the Bogdanov map is applied $n_i$ times on the bit-plane $B_i$. Thereafter, the scrambled bit-planes $B_i$ are reorganised to construct the partially encrypted image $C_e$. The scrambling of the bit-planes changes the pixel

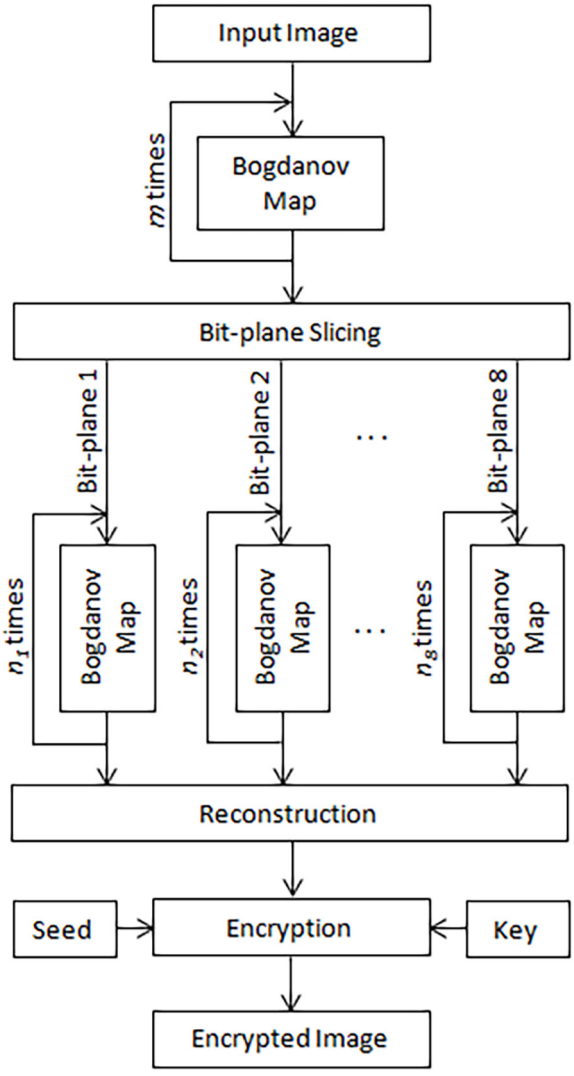


**Figure 1. Image encryption process.**

value and constructs the cipher image, $C_e$. To make the cipher image more robust to attacks $C_e$ is again encrypted using the keys generated by dyadic transform. The procedure for encryption is as given below and the process can be defined by Eq. (3) to Eq. (7).

### Encryption algorithm

*Input* : Plain image, *I*.
*Output* : Encrypted image or cipher image, *C*.
Procedure:

Step 1: Construct the scrambled image, $C_s$, by applying the Bogdanov map, *M*, *m* times on *I*, $m \le p$.

$$C_s = M(I, m) \tag{3}$$

Step 2: Separate the bit-planes of $C_s$. Let the bit-planes be $B_i$, $1 \le i \le 8$.

Step 3: Subject the bit-planes, $B_i$, to the Bogdanov map $n_i$ times, $n_i \le p$. Let the permuted bit-planes be, $B_{Si}$ $1 \le i \le 8$.

Step 4: Construct partially ciphered image, $C_e$, by reorganising the permuted bit planes, $B_{Si}$, $1 \le i \le 8$.

$$C_e = \mathrm{P}\left(\mathrm{M}\left(B_i(C_s), n_i\right)\right) \tag{4}$$

where *P* is the reconstruction function.

Step 5: Generate a key matrix, *K*, using dyadic transform (Pisarchik & Zanin 2010), $d:[0,1)\to[0,1)$ defined as

$$\delta(x) = \begin{cases} 2x & 0 \le x < 0.5 \\ 2x\text{-}1 & 0.5 \le x < 1 \end{cases} \tag{5}$$
$$x_{n+1} = \delta(x),\ n = 0,1,2,\cdots$$

with the condition if $x = 0$ or 1 then $x = x_0$, $x_0$ is the initial value.

Step 6: Encrypt $C_e$ by *K*.

$$C = E(C_e, K) \tag{6}$$

using (Chen et al. 2004)

$$C(x) = K(x) \oplus \left[I(x) + K(x)\right] mod\, G \oplus C(x-1) \tag{7}$$

where *E* is the encryption function, *G* is the value of color levels and *C*(0) is the *seed* for encryption.

The parameter *p* symbolizes the Bogdanov period, the number of iterations after which the image return to its original form. The parameter vector (*m*, $n_i$, *K*, *seed*), $1 \le i \le 8$, forms the symmetric key and controls the encryption process.

### Image Decryption

Since the proposed cryptosystem is a symmetric cipher, the decryption process is the inverse of the encryption process with the same parameter vector (*m*, $n_i$, *K*, *seed*), $1 \le i \le 8$ and can be defined as in Eq. (8) to Eq. (11). The image decryption process is shown in Figure 2. First, the cipher image, *C*, is decrypted by using *K* and *seed* to get the partially deciphered image $C_e$. $C_e$ is then separated into eight bit-planes, $B_{ei}$, $1 \le i \le 8$, and the inverse Bogdanov map is applied $n_i$ times on the bit-plane, $B_{ei}$ The unscrambled bit-planes of $B_{ei}$ are then reorgainsed to construct the scrambled image $C_S$. The image $C_S$ is, however, unintelligible as the pixels are not positioned in their original position. The inverse Bogdanov map is once again applied *m* times on $C_S$ to unscramble the image. The resultant will be the original image, *I*, provided the encrypted image is not subjected to attacks.

### Decryption algorithm

*Input :* Cipher image, *C*.
*Output :* Decrypted image or plain image, *I*.
*Procedure:*

Step 1: Decrypt *C* by *K* to get the partially deciphered image $C_e$.

$$C_e = \mathrm{D}(C, K) \tag{8}$$

using (Chen et al. 2004)

$$C_e(x) = \left[K(x) \oplus C(x) \oplus C(x-1) + G - K(x)\right] mod\, G \quad (9)$$

Step 2: Separate the bit-planes of $C_e$. Let the bit-planes be $B_{e_i}$, $1 \le i \le 8$.

Step 3: Subject the bit-planes $B_{e_i}$ to the inverse Bogdanov map, $M'$. Apply the map on the bit-planes, $B_{e_i}$, $n_i$ times, $n_i \le p$, $1 \le i \le 8$.

Step 4: Construct the scrambled image $C_s$, by reorganising the unscrambled bit planes, $B_i$, $1 \le i \le 8$.

$$C_s = P\left(M'\left(B_{e_i}(C_e), n_i\right)\right) \quad (10)$$

Step 5: Unscramble $C_s$ using the inverse Bogdanov map '$m$' times to get the plain image, $I$, $m \le p$.

$$I = M'(C_s, m) \quad (11)$$

## RESULTS AND DISCUSSION

The proposed cryptosystem abide by the basic principles of a chaotic cryptosystem: confusion and diffusion by changing both the position and value of the pixels. Both the operations take in permutation processes, where-in they take the advantage of the Bogdanov map. Unlike Arnold transform, which applies only to square images, Bogdanov map applies to images of arbitrary size. As the cryptosystem is symmetric, it uses the same set of keys for both encryption and decryption.

In the confusion phase, the input image is subjected to the Bogdanov map $m$ times. The Bogdanov map shuffles the pixel positions however does not change the value of the pixels. Its repeated application on the input image results in a scrawled image. Figure 3a-d depict the jet plane image of size 384 x 512, its histogram, the scrambled image and its histogram respectively. The scrambled image was obtained by applying Bogdanov map eight times ($m$ = 8) on the jet plane image when $k$ = 2. As a histogram reveals the distribution of pixel values with the image, it can be seen that

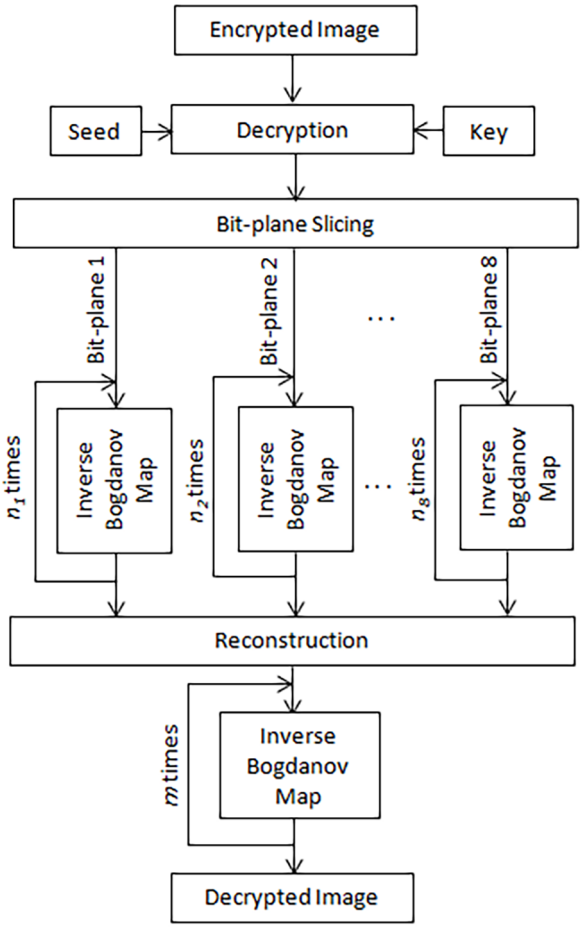


**Figure 2. Image decryption process.**

the frequencies of the pixels are not altered by the application of the Bogdanov map. The changed pixel positions, however, offer a visual perception of encryption.

The change in pixel positions weakens the correlation among the adjacent pixels in the image. The correlation distributions of the jet plane image and the scrambled image in horizontal, vertical and diagonal directions are plotted in Figure 4. It is evident that there is a high correlation among the adjacent pixels in the plain image, as the dots are located surrounding the diagonal in Figure 4a-c, whereas they are scattered over the entire plane in Figure 4d-f. The Lena image, its scrambled image for the same parameters ($k$ = 2 and $m$ = 8) and their

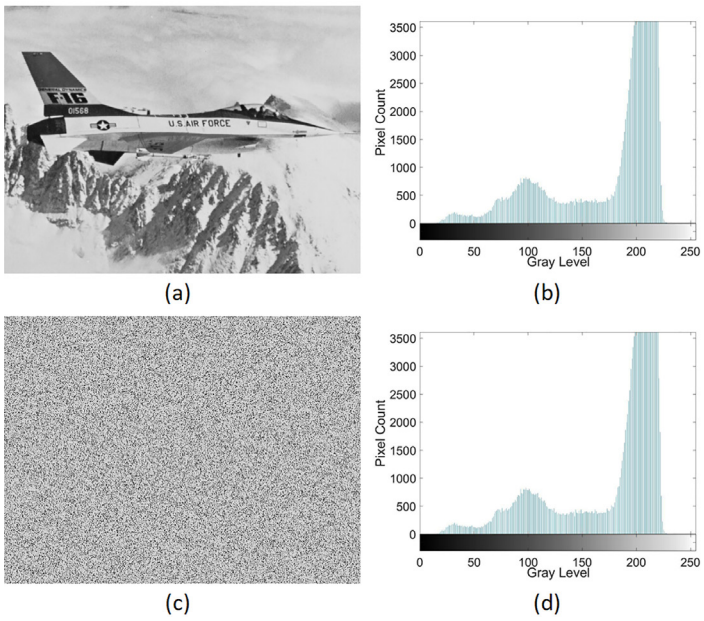


**Figure 3. (a) Jet plane image (b) Histogram of jet plane image (c) Scrambled jet plane image (d) Histogram of scrambled jet plane image.**

correlation distributions are plotted in Figure 5. Figure 5a-d depict the plain image and its correlation distribution in horizontal, vertical and diagonal directions respectively and Figure 5e-h for the scrambled image.

In the diffusion phase, the scrambled image is sliced into eight bit planes. In Figure 6a-h represents the bit-planes of the jet plane image and i-p represents the bit-planes of the scrambled image. Even though the corresponding bit planes of the original and scrambled image are not similar, the percentage of information provided by the $i^{th}$ bit of the pixels is the same. The computation (Zhu et al. 2011) is given by Eq. (12). The data pertaining to the same is listed in Table I.

$$p(i) = \frac{2^{i-1}}{\sum_{1}^{8} 2^{i-1}} \tag{12}$$

Thus, only the confusion phase is not enough to attain a good encryption as the actual information content of the image remains unaltered. Only the perceptual information apparent to the human eye differs.

Each bit-plane of the scrambled image was individually subjected to the Bogdanov map $n_i$ times, $1 \le i \le 8$. The image is reconstructed by reorganising the scrambled bit planes. As the $n_i$ are not the same for all the bit-planes, the bits of the pixels change, resulting in changes in the pixel value. At this stage, the image pixel positions and values are changed, resulting in an encrypted image. The encrypted jet plane image and the corresponding histogram are shown in Figure 7a, b respectively. The encrypted image was constructed with scrambled bit planes, where the bit planes 1 to 8, are subjected to Bogdanov map 5, 4, 8, 6, 5, 9, 3, 8 and 8 times respectively.

An ideal encrypted image should avert the adversary from extracting any meaningful information from it. Hence, to make it more robust, the resultant image was again subjected to encryption by the keys generated using dyadic transform presented in Step 5 of the encryption algorithm. The encryption process of each pixel encompasses the previous encrypted pixel with a randomly generated initial seed value. This leads to a change in the pixel values once again, culminating in a doubly encrypted image.

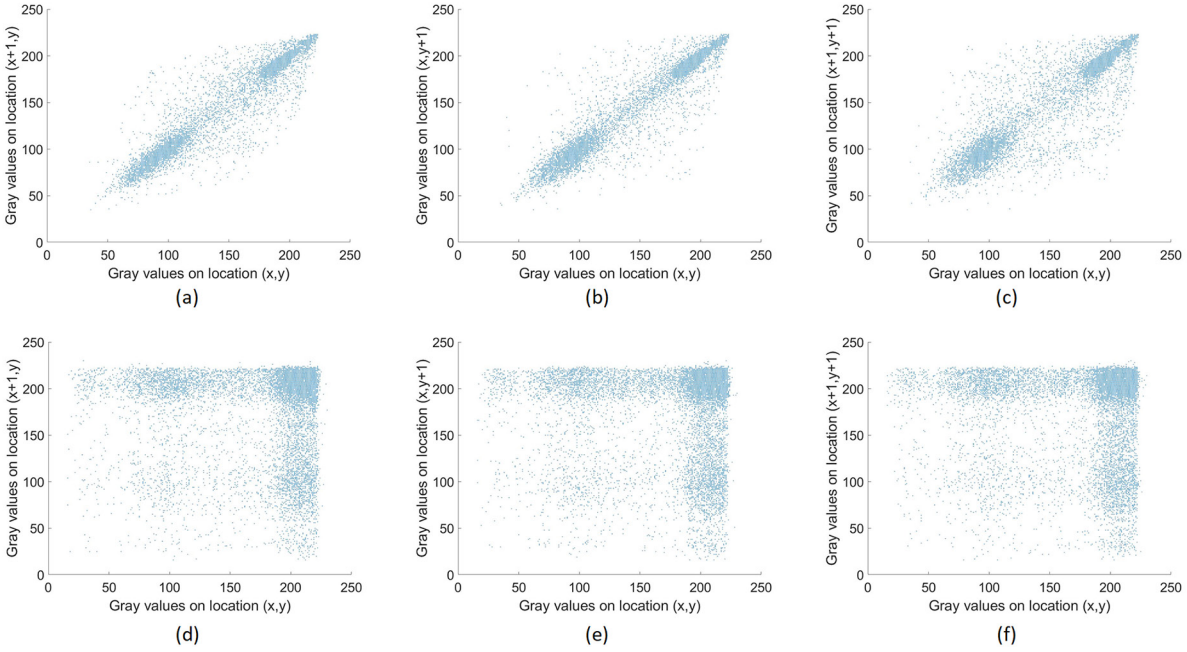


**Figure 4. Correlation distribution of adjacent pixels of the jet plane image in (a) horizontal (b) vertical (c) diagonal directions and the scrambled jet plane image in (d) horizontal (e) vertical (f) diagonal directions.**

Correlation is a measure of the relationship between the plain and the encrypted images (Amrane et al. 2016). When the images are totally different, the correlation coefficient equals zero. The correlation coefficients of image pixels in horizontal (H), vertical (V) and diagonal (D) directions of the given plain image and the corresponding encrypted image are shown in Table II. The table also presents the correlation coefficient between the plain and the encrypted images. Smaller the correlation, gives better encryption effect and higher the security (Shuqin et al. 2018).

A histogram graphically represents the frequency of distribution of pixel values within an image. Histogram analysis illustrates the quality of an encrypted image. A good image encryption method produces an encrypted image having uniformly-distributed histogram. The plain images listed in Table II, their histogram, the corresponding encrypted images and the respective histograms are depicted in Figure 8 a-e, f-j, k-o and p-t respectively.

The error in the encrypted image compared to that of the original image can be measured using MSE (Mean Square Error) metric (Al-Romema et al. 2012). The MSE is computed using the mathematical formula

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I(i,j)-C(i,j)\right]^2}{M \times N} \tag{13}$$

where *I* and *C* are the plain and cipher images of size *M x N* respectively. The values of the MSE and the error are directly proportional, that is the lower value of MSE indicates lesser error and the higher value of MSE indicates more error. The MSE measured during encryption is depicted in Table III. The MSE value increases with the processes of encryption resulting in a noisy image.

To acquire the information from the ciphered data, the adversary may observe the difference between the results after making

minor modifications on the encrypted image (Chen et al. 2004). This will help them to derive relationship between the plain and the encrypted image. If a trivial change in plain image causes significant variation in the encrypted image, makes these attacks inefficient. The number of pixels change rate (NPCR) and the unified averaged changing intensity (UACI) are the two most quantities used to evaluate the strength of the image encryption algorithms with respect to differential attacks (Wu et al. 2011). Let $C_1$ and $C_2$ be the two encrypted images corresponding to the plain images having a pixel difference between them. The NPCR measure the number of pixels which changes value between $C_1$ and $C_2$ in percentage whereas UACI measures the average intensity difference between $C_1$ and $C_2$ in percentage. The NPCR and UACI are defined by the equations Eq. (14) and Eq. (16) respectively.

$$NPCR = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \tag{14}$$

where

$$D(i,j) = \begin{cases} 0, & if C_1(i,j) = C_2(i,j) \\ 1 & if C_1(i,j) \neq C_2(i,j) \end{cases} \tag{15}$$

$$UACI = \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255 \times T} \times 100\% \tag{16}$$

where $(i, j)$ defines the position of the pixel and $T$ is the total number of pixels in the image.

The Lena image of size 512 x 512 is subjected to above test with one pixel variation at position (1,1). The pixel value at (1,1), 162 was changed to 163 by modifying the least significant bit from 0 to 1. i.e., "10100010" to "10100011". Then, the images are encrypted using the same set of parameters and key to get the cipher images $C_1$ and $C_2$ respectively. The value of the parameter $k$ = 2. The size of the key is same as the size of the image. The other parameters used for encryption are presented in Table IV.

The computed values of NPCR and UACI for the 5 rounds are compared with the results produced by (Zhu et al. 2011) and the same is presented in Table V and Table VI respectively. The results show that the proposed method performs better.

Also, the average time taken to execute the encryption algorithm is much lesser than that of Zhu's method. The average time taken by Zhu's method to encrypt the Lena image is 36.1 ms whereas the proposed system is 2.59 ms. The average was computed by encrypting the Lena image by each cryptosystem ten times.

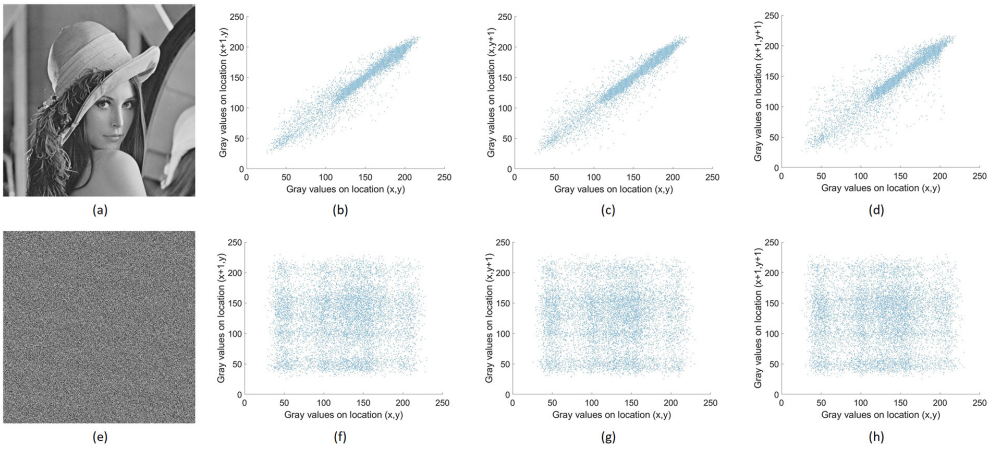


**Figure 5. Correlation distribution of adjacent pixels of the (a) Lena image in (b) horizontal (c) vertical (d) diagonal directions and the (e) scrambled Lena image in (f) horizontal (g) vertical (h) diagonal directions.**

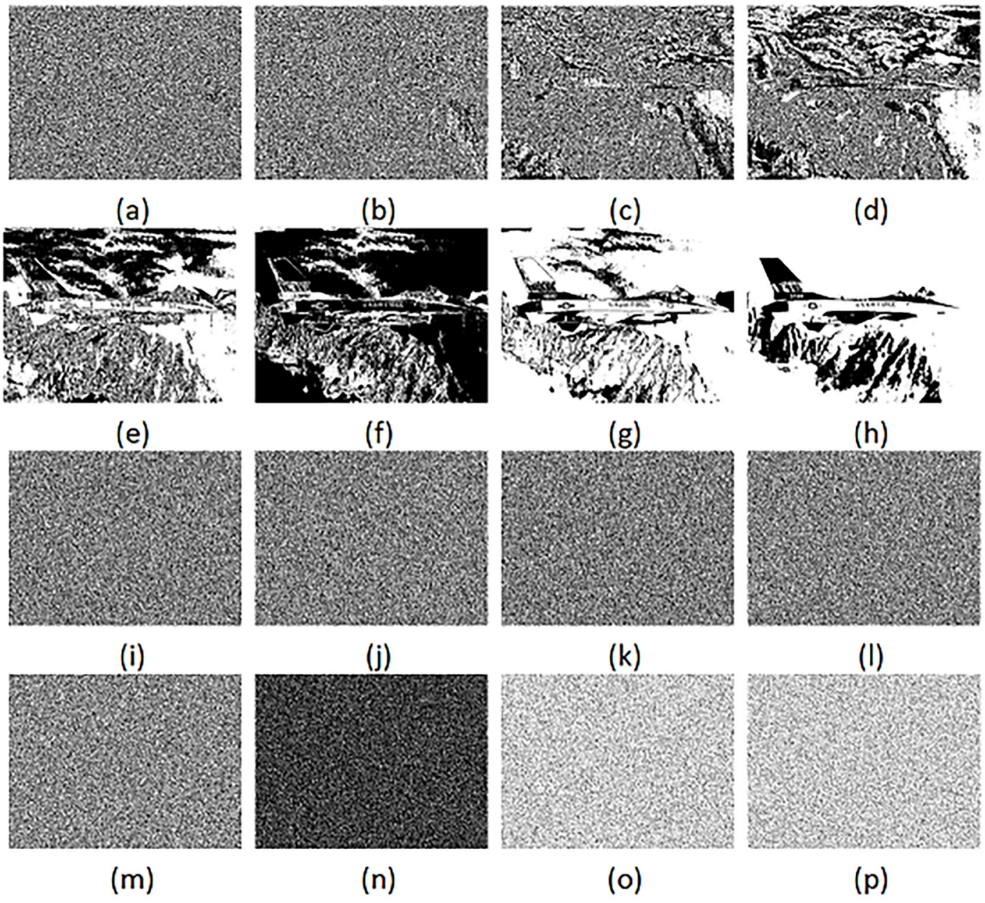


**Figure 6.** Eight bit planes of the jet plane image a-h and the scrambled image i-p in order.

**Table I.** Percentage of information provided by the bits of pixels.

| Bit position i in the pixel | Percentage of information contributed | |
|---|---|---|
| | Original image | Scrambled image |
| 1 | 0.2847 | 0.2847 |
| 2 | 0.5711 | 0.5711 |
| 3 | 1.1292 | 1.1292 |
| 4 | 2.3687 | 2.3687 |
| 5 | 4.9591 | 4.9591 |
| 6 | 4.3839 | 4.3839 |
| 7 | 28.8355 | 28.8355 |
| 8 | 57.4679 | 57.4679 |

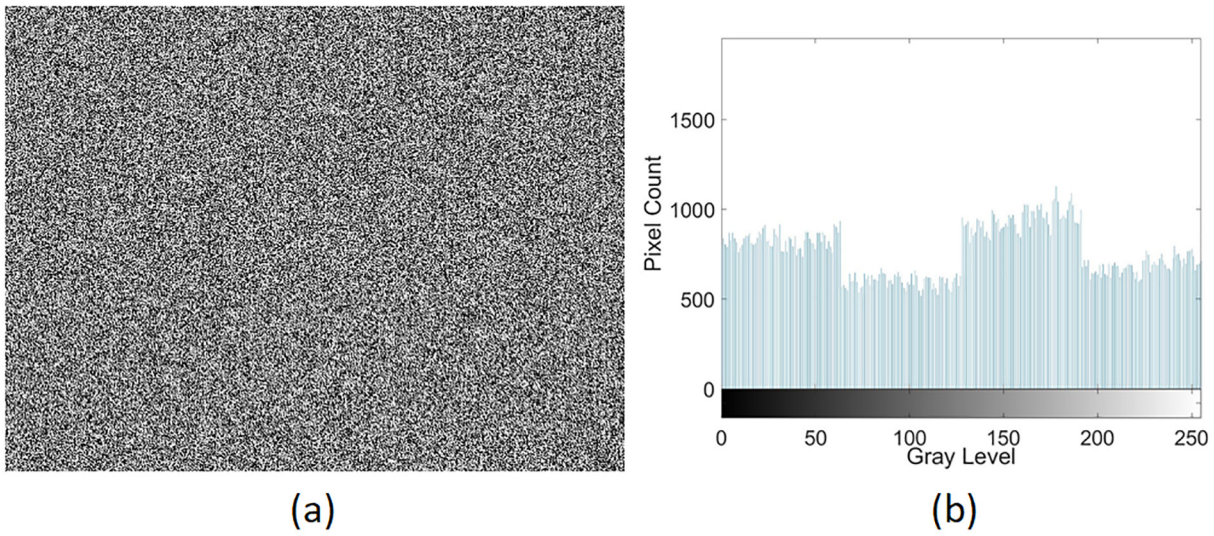


**Figure 7.** (a) Encrypted jet plane image after bit-plane scrambling and (b) its histogram.

**Table II.** Correlation Coefficients.

| Image | Size | Plain image (*I*) | | | Encrypted Image (*C*) | | | Correlation Coefficient between *I* and *C* |
|---|---|---|---|---|---|---|---|---|
| | | H | V | D | H | V | D | |
| Jet plane | 384 × 512 | 0.9688 | 0.9719 | 0.9465 | -0.0004 | -0.0027 | -0.0012 | 0.0014 |
| Cameraman | 128 × 128 | 0.9203 | 0.8658 | 0.8318 | -0.0483 | 0.0075 | -0.0019 | -0.0057 |
| Lena | 256 × 256 | 0.9593 | 0.9258 | 0.9037 | 0.00008 | -0.00004 | 0.0019 | -0.000009 |
| Mandril | 512 × 512 | 0.9123 | 0.9337 | 0.8669 | -0.0081 | 0.0017 | 0.0015 | 0.0008 |
| Peppers | 512 × 384 | 0.9793 | 0.9783 | 0.9686 | 0.0065 | -0.0026 | -0.0018 | -0.0020 |

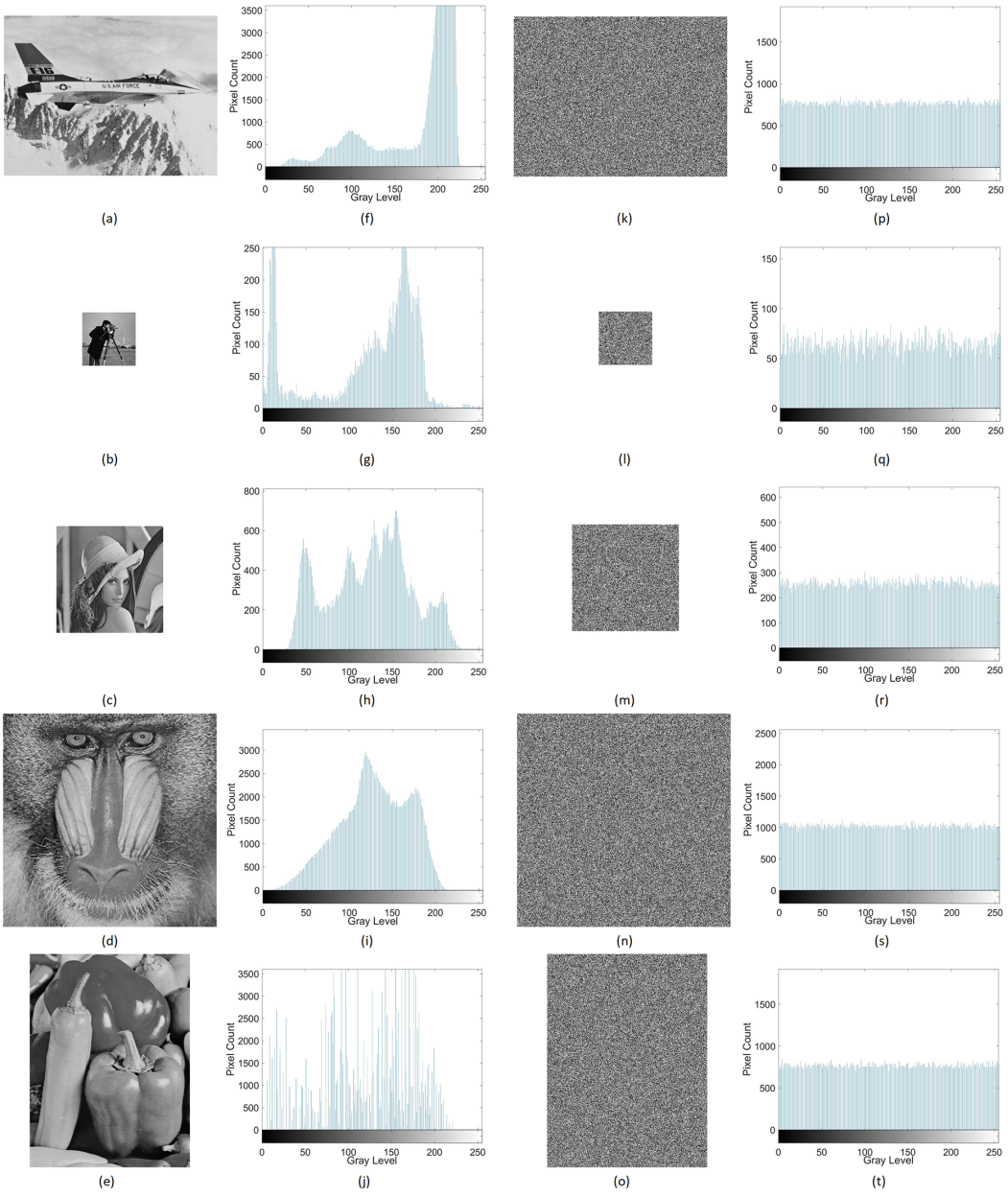


**Figure 8.** Plain images (a) Jet plane (b) Cameraman (c) Lena (d) Mandril (e) Peppers, (f-j) their histograms, (k-o) corresponding encrypted images and (p-t) the histograms of encrypted images.

**Table III.** Mean Square Error.

| Steps during encryption of jet plane image | MSE |
|---|---|
| After confusion | 4961.3 |
| After diffusion | 10269.0 |

**Table IV.** Encryption Parameters.

| Round | Parameters | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $m$ | $n_1$ | $n_2$ | $n_3$ | $n_4$ | $n_5$ | $n_6$ | $n_7$ | $n_8$ | *seed* |
| 1 | 7 | 8 | 7 | 4 | 7 | 2 | 7 | 1 | 3 | 25 |
| 2 | 8 | 7 | 3 | 10 | 1 | 4 | 4 | 8 | 8 | 125 |
| 3 | 4 | 6 | 7 | 8 | 3 | 7 | 7 | 2 | 1 | 245 |
| 4 | 3 | 6 | 2 | 8 | 3 | 5 | 7 | 9 | 10 | 35 |
| 5 | 1 | 3 | 8 | 3 | 8 | 2 | 9 | 3 | 2 | 157 |

**Table V.** NPCR.

| Round | Proposed | Zhu's |
|---|---|---|
| 1 | 63.3522 | 0.4222 |
| 2 | 99.6555 | 81.1958 |
| 3 | 99.6220 | 99.6051 |
| 4 | 99.6208 | 99.5933 |
| 5 | 99.6208 | 99.6273 |

**Table VI.** UCAI.

| Round | Proposed | Zhu's |
|---|---|---|
| 1 | 0.2484 | 0.1365 |
| 2 | 34.2885 | 27.3860 |
| 3 | 33.4515 | 33.3999 |
| 4 | 33.4475 | 33.4793 |
| 5 | 33.5269 | 33.4815 |

## CONCLUSION

A chaos-based simple image cryptosystem is proposed, using the Bogdanov map to accomplish the permutation process both at the pixel level and bit-level. In the confusion phase, the pixel positions are shuffled. The pixel values are modified twice in the diffusion phase: once by shuffling the bits of the bit-plane using Bogdanov map followed by encryption with the keys generated using dyadic transform. As a result, the permutation has the effects of both confusion and diffusion, and employs the Bogdanov map for permutation (shuffling). The cryptosystem is simulated using Matlab and its performance analysed. The result of the analysis shows that the proposed double image encryption model is simple, fast and secure with a sufficiently large keyspace. This guarantees its use in real-time image transmission and in e-commerce transactions.

## REFERENCES

ABDEIHALEEM SH, RADWAN AG & ABD-EL-HAFIZ SK. 2014. A chess-based chaotic block cipher. In: New Circuits and Systems Conference (NEWCAS), 12th International ed., IEEE, 405-408.

ABUNDIZ-PÉREZ F, CRUZ-HERNÁNDEZ C, MURILLO-ESCOBAR M & LÓPEZ-GUTIERREZ R. 2014. Fingerprint image encryption based on Rossler map. In: Proceedings of the International Conference on Communications, Signal Processing and Computers, 193-197.

AGILANDEESWARI L & GANESAN K. 2016. A robust color video watermarking scheme based on hybrid embedding techniques. Multimed Tools Appl 75(14): 8745-8780.

AL-ROMEMA NA, MASHAT AS & ALBIDEWI I. 2012. New chaos-based image encryption scheme for RGB components of color image. Comput Sci Eng 2(5): 77-85.

ALVAREZ G & LI S. 2006. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcat Chaos 16(08): 2129-2151.

AMRANE H, ZOUHIR M, KAMAL EM & ABDELMALIK B. 2016. A novel binary image encryption algorithm based on diffuse representation. Eng Sci Technol Int J 19(4): 1887-1894.

ARROWSMITH DK, CARTWRIGHT JH, LANSBURY AN & PLACE CM. 1993. The Bogdanov map: Bifurcations, mode locking, and chaos in a dissipative system. Int J Bifurcat Chaos 3(4): 803-842.

BAPTISTA MS. 1998. Cryptography with chaos. Phys lett A 240(1-2): 50-54.

CHEN G, MAO Y & CHUI CK. 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Soliton Fract 21(3): 749-761.

GONZALES OA, HAN G, DE GYVEZ JP & SÁNCHEZ-SINENCIO E. 2000. Lorenz-based chaotic cryptosystem: a monolithic implementation. IEEE Trans Circuits Syst I: Fundam Theory Appl 47(8): 1243-1247.

GUO W, ZHAO J & YE R. 2014. A chaos-based pseudorandom permutation and bilateral diffusion scheme for image encryption. Int J Image Graphics Signal Process 6(11): 50-61.

KOCAREV L & LIAN S. 2011. Chaos-based cryptography: Theory, algorithms and applications. Studies in Computational Intelligence. Springer 354: 398.

KUMAR GS, BAGAN KB & VIVEKANAND V. 2011. A novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD] utilizing duo chaos mapping applicability in wireless systems. Procedia Comput Sci 3: 378-387.

PISARCHIK AN, FLORES-CARMONA NJ & CARPIO-VALADEZ M. 2006. Encryption and decryption of images with chaotic map lattices. Chaos: J Nonlinear Sci 16(3): 033118.

PISARCHIK AN & ZANIN M. 2008. Image encryption with chaotically coupled chaotic maps. Phys D: Nonlinear Phenom 237(20): 2638-2648.

PISARCHIK AN & ZANIN M. 2010. Chaotic map cryptography and security. In: Encryption: Methods, Software and Security. Nova Science Publishers Inc, 1-28.

RADWAN AG, ABDELHALEEM SH & ABD-EL-HAFIZ SK. 2016. Symmetric encryption algorithms using chaotic and non-chaotic generators: a review. J Adv Res 7(2): 193-208.

RADWAN AG, SOLIMAN AM & EL-SEDEEK A. 2004. MOS realization of the modified Lorenz chaotic system. Chaos Soliton Fract 21(3): 553-561.

RUN-HE Q, YUN C & YU-ZHEN F. 2011. Integrated confusion-diffusion mechanisms for chaos based image encryption. In: Image and Signal Processing (CISP), 4th ed., International Congress, IEEE 2: 629-632.

SHUQIN Z, CONGXU Z & WENHONG W. 2018. A new image encryption algorithm based on chaos and secure hash SHA-256. Entropy 20(9): 716-718.

SOM S & SEN S. 2013. A non-adaptive partial encryption of grayscale images based on chaos. Proc Tech 10: 663-671.

SUN F, LIU S, LI Z & LÜ Z. 2008. A novel image encryption scheme based on spatial chaos map. Chaos Soliton Fract 38(3): 631-640.

WU X, LI Y & KURTHS J. 2015. A new color image encryption scheme using CML and a fractional-order chaotic system. PloS ONE 10(3): 28.

WU Y, NOONAN JP & AGAIAN S. 2011. NPCR and UACI randomness tests for image encryption. J Sel Area Telecommun 1(2): 31-38.

YE R. 2011. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Opt Commun 284(22): 5290-5298.

ZANIN M & PISARCHIK AN. 2014. Gray code permutation algorithm for high-dimensional data encryption. Inform Sciences 270: 288-297.

ZHANG W, WONG KW, YU H & ZHU ZL. 2012. An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion. Opt Commun 285(9): 2343-2354.

ZHANG W, WONG KW, YU H & ZHU ZL. 2013. A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Commun Nonlinear Sci 18(3): 584-600.

ZHANG X, SHAO L, ZHAO Z & LIANG Z. 2014. An image encryption scheme based on constructing large permutation with chaotic sequence. Comput Electr Eng 40(3): 931-941.

ZHANG Y & XIAO D. 2014. Self-adaptive permutation and combined global diffusion for chaotic color image encryption. AEU-Int J Electron C 68(4): 361-368.

ZHU ZL, ZHANG W, WONG KW & YU H. 2011. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inform Sciences 181(6): 1171-1186.

**How to cite**
SUBASHINI V. JANARDHANAN & POORNACHANDRA SANJEEVA.. 2020. Bogdanov Map-based Permuted Double Image Encryption. An Acad Bras Cienc 92: e20181207. DOI. 10.1590/0001-3765202020181207.

*Manuscript received on October 31, 2017;*
*accepted for publication on March 5, 2019*

**SUBASHINI V. JANARDHANAN**[1]
https://orcid.org/0000-0002-3151-0068

**POORNACHANDRA SANJEEVA**[2]
https://orcid.org/0000-0003-2804-6329

[1]Department of Computer Science and Engineering, Jerusalem College of Engineering, Tambaram-Velachery Main Road, Narayanapuram, Pallikkaranai, Chennai, 600 100 Tamil Nadu, India

[2]Department of Electronics and Communication Engineering, Excel Engineering College, NH-544 Salem Main Road, Sankari West (Post), Pallakkapalayam, Near Komarapalayam (Village), Namakkal, 637 303, Tamil Nadu, India

Correspondence to: **V.J. Subashini**
*E-mail: vjsubashini@yahoo.co.in*

## Author contributions

V.J. Subashini and S. Poornachandra conceived the idea of the image cryptosystem presented in this paper. Subashini developed the theory and did the implementation. Poornachandra supervised and reviewed the findings. Both the authors contributed to the final manuscript.

CC BY